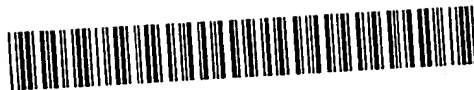


(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 289 188 A3

(12)

EUROPEAN PATENT APPLICATION(51) Int Cl.7: **H04L 9/18**

(88) Date of publication A3:
16.07.2003 Bulletin 2003/29

(43) Date of publication A2:
05.03.2003 Bulletin 2003/10

(21) Application number: **02254773.1**

(22) Date of filing: **08.07.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **24.08.2001 US 314684 P**
20.12.2001 US 26109

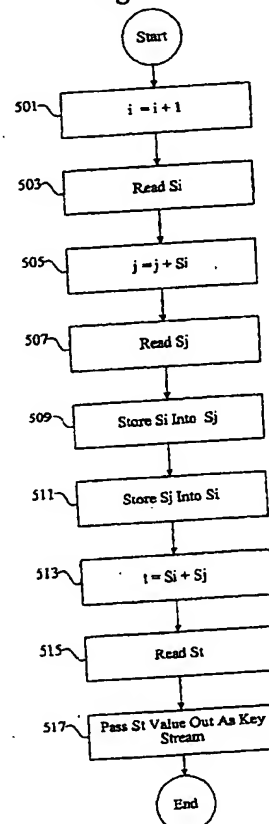
(71) Applicant: **Broadcom Corporation**
Irvine, CA 92619-3616 (US)

(72) Inventor: **Matthews, Donald P., Jr.**
Morgan Hill, CA 95037 (US)

(74) Representative: **Jehle, Volker Armin, Dipl.-Ing.**
Patentanwälte
Bosch, Graf von Stosch, Jehle,
Flügggenstrasse 13
80639 München (DE)

(54) **Methods and apparatus for accelerating ARC4 processing**

(57) Methods and apparatus are provided for improving ARC4 processing in a cryptography engine. A multiple ported memory can be used to allow pipelined read and write access to values in memory. Coherency checking can be applied to provide that read-after-write and write-after-write consistency is maintained. Initialization of the memory can be improved with a reset feature occurring in a single cycle. Key shuffle and key stream generation can also be performed using a single core.

Fig. 5**EP 1 289 188 A3**



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 25 4773

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	KUNDAREWICH P D ET AL: "A CPLD-based RC4 cracking system" ELECTRICAL AND COMPUTER ENGINEERING, 1999 IEEE CANADIAN CONFERENCE ON EDMONTON, ALTA., CANADA 9-12 MAY 1999, PISCATAWAY, NJ, USA, IEEE, US, 9 May 1999 (1999-05-09), pages 397-402, XP010359792 ISBN: 0-7803-5579-2	13,17-20	H04L9/18
Y		1,2,5-9, 11,14 3,4,10, 12,15, 16,21-28	
A	* abstract *		
	* page 398, left-hand column, line 24 - line 34 *		
	* page 398, right-hand column, line 5 - line 52 *		
	* page 400, right-hand column, line 12 - line 21 *		
	* page 401, right-hand column, line 4 - line 7; figures 1,3 *		
Y	---		
Y	US 6 088 800 A (JONES DAVID E ET AL) 11 July 2000 (2000-07-11)	1,2,5-9, 11,14 3,4,10, 12,13, 15-28	H04L G11C
A	* abstract *		
	* column 3, line 4 - line 65 *		
	* column 6, line 3 - line 52 *		
	* column 11, line 22 - line 24; figure 2 *		
A	---		
A	US 4 737 933 A (CHIANG MICHAEL ET AL) 12 April 1988 (1988-04-12)	1-28	
	* abstract *		
	* column 1, line 57 - column 2, line 18; figure 3 *		

The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 22 May 2003	Examiner Post, K
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 (03.02) (P04001)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 02 25 4773

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-05-2003

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 6088800	A	11-07-2000	WO	9944329 A2	02-09-1999
			DE	19983127 T0	10-05-2001
			FR	2778519 A1	12-11-1999
			GB	2350218 A ,B	22-11-2000
			GB	2381913 A	14-05-2003
			JP	2002505451 T	19-02-2002
			US	6434699 B1	13-08-2002

US 4737933	A	12-04-1988	CA	1207916 A1	15-07-1986
			EP	0137808 A1	24-04-1985
			JP	60500589 T	25-04-1985
			WO	8403377 A1	30-08-1984

EPO FORM P4458

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE BLANK (USPTO)